แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

- ☒ Financial Damage
- ☒ Reputation Damage
- ☒ Non-compliance
- ☒ Privacy Violation

ผลกระทบต่อระบบ

- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability

TLP Color : CLEAR

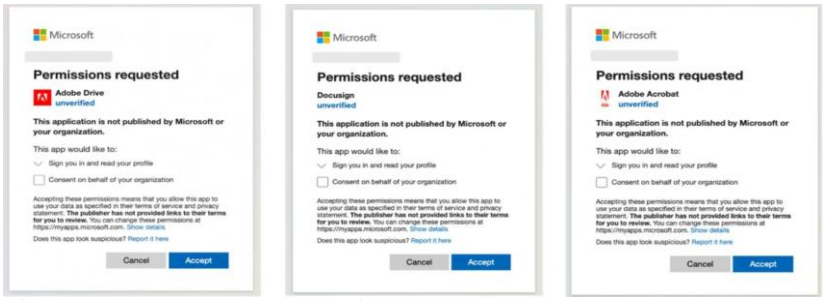
ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือน Malicious Open Authentication App. ขโมยบัญชี Microsoft O365

วันที่แจ้งเตือน 17 มีนาคม 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (“สำนักงาน ก.ล.ต.”) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (“TCM-CERT”) ได้ติดตามข่าวสารเกี่ยวกับการโจมตีทางไซเบอร์ พบรายงานของ Proofpoint ผู้ให้บริการด้านความปลอดภัยทางไซเบอร์ กรณี พบผู้ไม่ประสงค์ดีได้สร้างแอปพลิเคชัน Microsoft Oauth ปลอม (Malicious Apps) ที่แอบอ้างเป็นแอปพลิเคชัน Adobe Drive, Adobe Drive X, Adobe Acrobat และ DocuSign โดย Malicious Apps นี้ จะร้องขอสิทธิในการเข้าถึงข้อมูลทั่วไป เพื่อไม่ให้ผิดสังเกต เช่น profile, email และ OpenID เป็นต้น เมื่อผู้ใช้อนุญาตให้ Malicious Apps เข้าถึงข้อมูล ระบบจะเปลี่ยนเส้นทางไปยังเว็บไซต์ฟิชชิ่งที่ออกแบบให้ดูเหมือนหน้าล็อกอินของ Microsoft O365 หากผู้ใช้งานไม่ระวังและกรอกข้อมูลลงในหน้าล็อกอินปลอมดังกล่าว ทำให้ผู้ไม่หวังดีสามารถขโมยบัญชีผู้ใช้งาน และอาจเข้าถึงระบบ ส่งผลให้เกิดความเสียหายทางธุรกิจได้ ดังภาพตัวอย่าง



นอกจากนี้ Proofpoint รายงานว่าอาจมีการติดตั้งมัลแวร์โดยใช้เทคนิค ClickFix social engineering attack โดยหลอกให้ผู้ใช้งานดำเนินการผ่านกระบวนการ “human verification” โดยใช้งาน CAPTCHA ที่เป็นอันตราย (Malicious CAPTCHA) ส่งผลให้ผู้ไม่หวังดีส่งคำสั่งผ่านเมนู Run ของ Windows และดำเนินการ Execute คำสั่งในเครื่องของผู้ใช้งานเพื่อติดตั้งมัลแวร์ได้ในที่สุด

อย่างไรก็ดี พบว่า OAuth ยังคงเป็นวิธีที่มีประสิทธิภาพในการขโมยข้อมูลบัญชี Microsoft O365 ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยไซเบอร์ขององค์กรได้

การดำเนินมาตรการเบื้องต้น เมื่อพบว่ามีการอนุญาตการใช้งาน Malicious Oauth Apps แล้ว องค์กรควรพิจารณาดังนี้

1) ตรวจสอบและเพิกถอนแอป Oauth ที่ไม่รู้จัก เพื่อป้องกันการเข้าถึงที่ไม่พึงประสงค์ โดยไปที่ ‘My Apps’ (myapplications.microsoft.com) ⟶ 'Manage your apps' ⟶ และเพิกถอนแอป OAuth ที่ไม่รู้จัก
2) ผู้ดูแลระบบ Microsoft 365 ควรจำกัดสิทธิการอนุมัติแอปของบุคคลที่สาม เพื่อป้องกันการให้สิทธิโดยไม่ได้รับอนุญาต โดยไปที่ ‘Enterprise Applications' ⟶ 'Consent and Permissions' ⟶ set ‘Users can consent to apps' to 'No.’
3) พนักงานควรได้รับการฝึกอบรมให้ระมัดระวังคำขออนุญาตจากแอป ตรวจสอบแหล่งที่มาก่อนอนุมัติ และไม่คลิกลิงก์ที่น่าสงสัย
4) การเปิดใช้งาน MFA สำหรับบัญชีทั้งหมดช่วยลดความเสี่ยงแม้รหัสผ่านรั่วไหล
5) การตรวจสอบกิจกรรมที่น่าสงสัยในบันทึกของ Microsoft 365 และ
6) ตั้งค่าการแจ้งเตือนสำหรับการล็อกอินจากตำแหน่งหรืออุปกรณ์ใหม่ช่วยเพิ่มการเฝ้าระวัง หากพบว่าบัญชีถูกบุกรุก ควรรีเซ็ตรหัสผ่าน เพิกถอนแอปที่ไม่รู้จัก ตรวจสอบกิจกรรมย้อนหลัง และรายงานต่อทีมรักษาความปลอดภัยขององค์กรทันที

สำนักงาน ก.ล.ต. และ TCM-CERT เล็งเห็นถึงความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดต่อผู้ประกอบธุรกิจในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบธุรกิจทราบและพิจารณาดำเนินการตามความเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจจะเกิดขึ้นกับการปฏิบัติงานของบริษัท

ข้อมูลอ้างอิง

1. https://www.bleepingcomputer.com/news/security/malicious-adobe-docusign-oauth-apps-target-microsoft-365-accounts/
2. https://cybersecuritynews.com/microsoft365-themed-attack-leveraging-oauth-redirection/